基于条件变分自编码的密码攻击算法 *

段大高 [a,b]，赵振东 [a]，梁少虎 [a]，韩忠明 [a,b]

(北京工商大学 a.计算机与信息工程学院; b.食品安全大数据技术北京市重点实验室，北京 100048)

摘　要： 密码是数据加密和用户认证的普遍方式，用户设置的密码并不完全是随机性的，因此很容易受到密码破解工具的攻击。使用密码猜测算法是评估用户密码强度和安全性的有效方法，提出一种基于条件变分自编码密码猜测算法 PassCVAE。本算法基于条件变分自编码模型，将用户个人信息作为条件特征，训练密码攻击模型。在编码器端，分别使用双向 GRU 循环神经网络和 TextCNN 文本卷积神经网络，实现对密码序列和用户个人信息的编码和特征的抽象提取；在解码器端使用两层 GRU 神经网络，实现对用户个人信息和密码数据隐编码的解码，生成密码序列。本算法可以有效地拟合密码数据的分布和字符组合规律，生成高质量的猜测密码数据。多组实验结果表明，提出的 PassCVAE 算法优于现有的主流密码猜测算法。

关键词： 条件变分自编码；密码猜测算法；密码攻击

中图分类号： TN918.4　　doi: 10.19734/j.issn.1001-3695.2018.08.0649

Password cracking algorithm using conditional variational auto-encoders

Duan Dagao[a,b], Zhao Zhendong[a], Liang Shaohu[a], Han Zhongming[a,b]

(*a. School of Computer & Information Engineering, b. Beijing Key Laboratory of Big Data Technology for Food Safety, Beijing Technology & Business University, Beijing* 100048, *China*)

Abstract: Passwords are universal methods for data encryption and user authentication. The passwords set by users are not completely random. Therefore, the passwords are easily guessed and attacked by password crackers. Using a password guessing algorithm is an effective way to assess the strength and security of a password. This paper proposes PassCVAE based on conditional variation auto-encoding (CVAE) model. The algorithm take user's personal information as the conditional feature to train the password attack model. For the encoder, bidirectional GRU recurrent neural network and Text Convolution Neural Network (TextCNN) are used to extract the feature of the password sequence and personal information **Abstract:** y. The decoder uses two layers of GRU neural network to generate a password sequence based on the corresponding feature of personal information and hidden coding of password. The algorithm can effectively fit the distribution of password data, learn character combination rules and generate high-quality password guessing data. Multiple sets of experiments show that the proposed PassCVAE is better than the existing password guessing algorithms.

Key words: conditional variational auto-encoders; password guessing algorithm; passwords cracking

0　引言

随着移动互联网技术的快速发展和广泛普及，越来越多的用户通过移动终端学习、工作和娱乐。有效、安全的用户身份验证对网络信息安全和用户隐私数据保护至关重要。虽然有最新提出的指纹密码识别、人脸识别等技术，但是用户密码仍是最普遍的认证方式，主要是因为实现操作简单、用户体验良好和软件系统开发代价较小。不幸的是，多个密码数据库泄露表明用户倾向选择容易猜到的密码，主要由常见的字符串和数字组成，并且有不少密码创建规则中包含多种多样的个人信息组合方式,所以容易受到密码破译算法攻击。因此确认用户密码设置是否安全，是一个十分重要的安全问题，主动在线密码猜测检测技术常常用于评估密码强度。许多学者提出，基于概率统计模型的在线密码猜测算法，来验证用户密码的安全性。文献[1]对大量概率密码模型进行了系统的评估，包括使用多种归一化和平滑的马尔可夫模型。文献[2]提出了新的基于马尔可夫模型的密码破解器，显著提高了现有算法的猜测速度。文献[3]提出一种最高概率顺序生成密码结构的方法，首先根据已有的公开数据集训练自动创建上下文无关的语法，然后根据学习到的语法，生成单词修改规则，用于生成猜测的密码。但是这些传统的统计方法无法准确地学习到用户的密码设置习惯，同时需要耗费大量的计算资源和时间代价，因此不适合实时密码强度评估。而且大部分现有的密码安全性检测算法，只考虑了密码数据集中字符放入的概率分布，并没有把用户个人信息（如邮箱、用户名等）纳入特征作为条件，而这些个人信息往往与密码有很强的相关性。

近年来深度学习[4,5]在人工智能领域取得显著成就。深度学习可以对抽象特征进行提取，并且拥有对高维数据强大的拟合的能力，也被证明在序列生成任务[6,7]中非常有效，本文利用深度学习中条件变分自编码(conditional variational autoencoders，CVAE)技术，将用户个人信息作为密码生成条

收稿日期： 2018-08-12；**修回日期：** 2018-10-17　**基金项目：** 国家教育部人文社会科学研究青年基金资助项目(13YJC860006)；国家自然科学基金资助项目(61170112，61532006)；北京市自然科学基金资助项目(4172016)

作者简介： 段大高（1976-），男，湖南新邵人，副教授，博士，主要研究方向为多媒体、数据挖掘（duandg@th.btbu.edu.cn）；赵振东（1990-），男，河南安阳人，硕士研究生，主要研究方向为数据挖掘；梁少虎（1992-），男，河南南阳人，硕士研究生，主要研究方向为数据挖掘；韩忠明（1972-），男，山西太原人，副教授，博士，主要研究方向为数据挖掘.

件来实现密码猜测任务，提出 PassCVAE 密码攻击算法，通过与多种现有模型在大规模数据集上进行对比实验，结果表明本文所提出的 PassCVAE 算法，性能优于现有传统密码猜测模型，可以更好地拟合数据分布，生成质量更高的猜测密码序列。

1　相关工作

最简单的密码攻击方法是暴力破解，即对所有可能组合进行彻底搜索。由于这种攻击方式所需的时间代价过于高，因此一般来说都是不可行的。作为暴力破解的改进，字典攻击逐一尝试用户自定义词典中的可能密码（单词或短语）。与暴力破解的不同，暴力破解会逐一尝试所有可能的组合密码，而字典式攻击会使用一个预先定义好的单词列表（可能的密码）。虽然有时这种简单的密码攻击方法可能会奏效，但仍然会有大量不是基于已有字典的密码组合会被遗漏，也不能准确地利用用户密码习惯的设置规则。为了解决这个问题，很多学者将机器学习引入密码猜测攻击模型中，以便更好地识别概率较高的密码字符组合和学习到密码文本数据的合理分布。文献[8]提出 TarGuess 密码攻击框架，借助上下文无关文法模型，建立了针对用户个人信息的文法自适应规则，利用贝叶斯优化方法取得了一定的研究成果。文献[9]借用多层循环神经网络 LSTM[10,11]实现概率语言模型，用以生成猜测密码，也取得了不错的攻击效果。文献[12]将马尔可夫模型引入字典攻击，显著减少了密码搜索空间，并提出了高效枚举剩余密码空间算法。文献[13]利用语法和语义标签构建上下文无关模型，捕获密码样本的语义本质。文献[14]针对中文密码，在上下文无关文法模型中添加了拼音规则，提升了算法效果。文献[15]通过统计分析 7000 万雅虎匿名密码数据集，提出新的评价指标代替香农熵和猜测熵。文献[16]提出了使用马尔可夫模型的自适应密码强度评价规则，大大提高了密码强度估计的准确性。文献[17]基于蒙特卡洛方法，提出了一种新方法来使用现代攻击方法需要的猜测次数，算法具有所用资源少、易收敛等优点。文献[18]基于暴力马尔可夫(BFM)，测量密码强度，BFM 是暴力破解和 n-gram 模型之间的混合体，可以较准确计算出所需猜测次数。文献[19]提出了一种基于对抗神经网络来增强密码生成的 PassGAN 新方法，通过现有的泄露密码数据，训练出一个对抗生成网络，PassGAN 可以近似逼近密码训练数据集分布情况，因此 PassGAN 可能匹配出尚未泄露的密码。

2　基于变分自编码的密码攻击算法

2.1　条件变分自编码

变分自编码(variational Autoencoder, VAE)是一种基于标准自编码模型正则化版本的生成模型。该模型将一个先验分布 $p(\bar{z})$ 强加到隐变量 $\bar{z}$ 上，$p(\bar{z})$ 是规整的几何形式(常取标准高斯分布)，使得模型能够生成更接近原始数据分布的样本。变分自编码(VAE)将标准自编码中的编码器替换为学习得到的后验识别模型 $q(\bar{z}|x)$，通常用神经网络做为编码器 $q(\bar{z}|x)$ 函数，参数化隐变量 $\bar{z}$ 的后验分布使其逼近强加的先验分布(标准高斯分布)。VAE 模型有两个学习目标：a)最小化样本的重构损失；b)最小化编码隐变量 $\bar{z}$ 和标准高斯分布的 KL 散度。模型的损失函数如式(1)所示，其中 $KL(q(\bar{z}|x)\|p(\bar{z}))$ 表示 $\bar{z}$ 的先验分布 $p(\bar{z})$ 和模型编码器后验分布 $q_\theta(\bar{z}|x)$ 之间的 KL 散度，度量的是两个分布中的相似度，当两个分布越相似时 KL 散度越小。

$$L(\theta;x)=-KL(q_\theta(\bar{z}|x)\|p(\bar{z}))+\mathbb{E}_{q_{\theta(\bar{z}|x)}}[\log p_\theta(x|\bar{z})] \tag{1}$$

$\mathbb{E}_{q_{\theta(z|x)}}[\log p_\theta(x|z)]$ 代表解码器 $p_\theta(x|z)$ 对数据样本的重构损失，模型的解码器学习目标是尽量还原真实数据。

条件变分自编码(CVAE)[20,21]是变分自编码的条件概率版本扩展，VAE 无法控制数据的生成过程，CVAE 通过给模型加上生成条件，可以生成特定条件下的生成数据。损失函数如式(2)所示，其中 y 是条件变量，解码器会在条件 y 下生成特定的数据。在本文密码猜测模型中取生成条件 y 为用户的个人信息，包括用户名、邮箱地址和电话号码等。

$$L(\theta;x,y)=-KL(q_\theta(\bar{z}|x,y)\|p(\bar{z}))+\mathbb{E}_{q_{\theta(z|x,y)}}[\log p_\theta(x|z,y)] \tag{2}$$

2.2　密码攻击模型

模型整体框架如图 1 所示，编码器 $q_\theta(\bar{z}|x,y)$ 由一个两层双向的 GRU 和一个 CNN 卷积网络两部分组成，GRU 编码器用来对用户密码序列进行编码，CNN 编码器用来对用户个人信息进行编码。

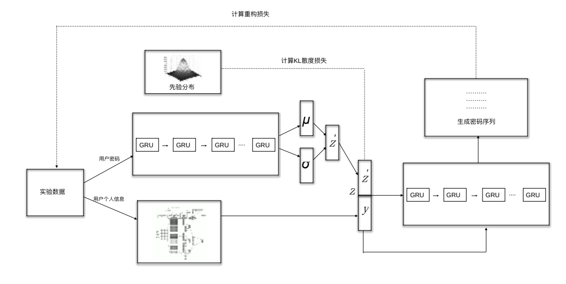


图 1　密码攻击模型示意图

Fig. 1　The overview of password cracking algorithm

如式(3)所示，$x_{1:t}$ 是用户的密码序列，$BiGRU$ 表示双向 GRU 循环神经网络，取其最后时刻输出状态 h_t 经过两个全连接层生成 μ 和 σ （式（4）（5））。在式(6)中 randn 代表从标准正态分布中采样出与 μ 同维度的随机向量，经过重参数化后得到中间编码 z'。式(7)中 g 是用户个人信息上下文数据，g ={用户名,邮箱地址,电话号码}，即把用户个人信息当作字符串串联起来，经过 CNN 卷积网络对其编码生成条件编码向量 y。式(8)将中间编码 z' 与条件编码 y 拼接在一起形成最终隐编码 z。

$$h_t=BiGRU_e(h_{t-1},x_{t-1}) \tag{3}$$

$$\mu=\tanh(w_\mu h_t) \tag{4}$$

$$\sigma=\tanh(w_\sigma h_t) \tag{5}$$

$$z'=\mathrm{randn}\cdot\mu+\sigma \tag{6}$$

$$y=\mathrm{CNN}(g) \tag{7}$$

$$z=[z',y] \tag{8}$$

模型解码器 $p_\theta(x|z,y)$ 由两层的单向的 GRU 的实现，如式(9)所示其每一个时刻的隐状态都加入了隐编码 z 和条件编码向量 y，$x'_{1:t}$ 是解码器网络生成的密码猜测序列。

$$h_t,x'_t=GRU_d([h_{t-1},y,z],x'_{t-1}) \tag{9}$$

在训练时，通过标准高斯先验分布，采用 KL 散度来控制编码器生成的隐编码 z，使之接近先验高斯分布。编码器 CNN 网络，将用户的个人信息(邮箱地址、用户名和电话号码)作为输入，生成用户的条件编码向量 y。最后将隐变量 z 和条件编码向量 y 拼接在一起作为解码器初始状态用以生成密码序列。

当模型训练结束后，在标准高斯分布中随机采样出隐变量 $\bar{z}$，用解码器 CNN 网络编码用户个人信息生成条件编码向

量 y 。将隐变量 $\bar{z}$ 和条件编码向量 y 输入解码器，就可以生成此用户的猜测密码序列。

编码器 $q_\phi(\bar{z}|x,y)$ 在先验分布的控制下，将数据集中的密码序列抽象编码填充在一个高维的高斯分布空间，在生成密码时，通过在 z 的先验分布 $p(\bar{z})$ 中采样出的隐变量，将符合训练数据的真实编码分布，结合条件编码向量 y，以此来生成用户密码猜测序列。

2.3 算法实现步骤

根据前面介绍的条件变分自编码和密码攻击模型，课整理得到算法 PassCVAE 的实现流程，如下所示。

算法 基于条件变分自编码的密码攻击算法

1：初始化 $BiGRU_e$ 和 CNN 编码器模块参数，初始化解码器 GRU_d 参数

2：**for** each iteration i=1,2,…, M **do**

3: 采样一个密码样本序列 $\boldsymbol{x}$ ，其用户上下文信息为 $\boldsymbol{g}$

4: 根据式(3)生成密码序列隐状态序列 $\boldsymbol{h}_1$, $\boldsymbol{h}_2$,… , $\boldsymbol{h}_t$

5: 根据式(4),(5)依据 h_t 生成变分参数 μ 和 σ

6: 根据式(6)得到密码序列编码隐变量 $\boldsymbol{z}'$

7: 根据式(7)得到用户上下文特征变量 $\boldsymbol{y}$

8: 根据式(8)生成最终隐变量 $\boldsymbol{z}$

9: 根据式(9)得到生成密码序列 $\boldsymbol{x}'$

10: 计算 $BiGRU_e$, CNN 和 GRU_d 模块的梯度

11: 更新 $BiGRU_e$, CNN 和 GRU_d 模块的参数

12: **end for**

3 实验与分析

3.1 数据集

本文实验评估数据集由三个大型真实密码数据集构成，数据集主要黑客攻击或者内部人员泄露并且已在互联网上可以公开获取。数据集具体描述如表 1 所示。

表 1 实验数据集

Tabel 1 Summary of datasets

数据集	训练集样本量	测试集样本量	每条记录所包含信息
12306	104400	27253	密码，邮箱，电话，身份证号，姓名
CSDN	621356	98700	密码，用户名，邮箱
人人网	476860	39476	密码，邮箱

12306 是中文互联网火车票订票平台泄露的密码数据，其中包含较完整的用户个人信息如用户邮箱、电话、身份证号、姓名(拼音字母)。CSDN 是 IT 社区平台泄露的用户密码数据，包含密码、用户名和邮箱信息。人人网数据是中文社交平台泄露的用户密码数据，包含密码、邮箱信息。

3.2 实验设置

为验证方法有效性，本文选择四种密码猜测算法作比较，分别是 PCFG[3]，OMEN[2],PassGAN[17]和 PassLSTM。其中 PCFC 和 OMEN 是基于传统的统计方法，PassGAN 采用深度学习中的生成对抗网络实现，PassLSTM 基于 LSTM 循环神经网络的语言模型。

实验模型分别根据实验数据集训练样本训练出密码生成模型，在测试集中规定每个密码的破解尝试次数不超过限定次数，即在 1000、2000、3000、4000 和 5000 次尝试以内破解成功视为模型攻击成功，计算过程如式(10)~(12)所示。在式(10)中 $X'=x'_{1:n}$ 代表生成的生成的 n 个猜测序列。分别统计各模型在不同数据集测试样本上猜测次数的成功率。实验结果如表 2~4 所示。

在 12306 数据集当中，用户的个人信息较多，本文提出的 PassCVAE 模型可以提取出更多条件信息，比其他几个模型有较明显的优势，表现出更好的性能。但由于 12306 数据集样本量只有 10 万多条，各模型的破解成功率也不如 CSDN 和人人网数据集表现得好。在三个数据集上，本文提出的 PassCVAE 模型都取得了最佳结果，也证明了用户个人信息的条件嵌入对破解密码生成的有效性。

表 2 12306 数据集破解成功率

Table 2 Performance on 12306 test set

尝试次数	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
1000	1.364	2.025	1.049	2.227	**2.931**
2000	1.984	2.153	1.170	2.880	**3.995**
3000	2.355	3.515	1.706	3.394	**4.696**
4000	2.616	3.761	1.714	3.856	**5.371**
5000	3.280	4.282	1.746	4.282	**5.892**

表 3 CSDN 数据集破解成功率

Table 3 Performance on CSDN test set

尝试次数	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
1000	9.067	9.272	4.107	9.327	**9.497**
2000	9.752	9.533	4.639	9.605	**9.960**
3000	10.002	9.971	5.093	10.253	**10.382**
4000	10.195	10.074	5.621	10.480	**10.978**
5000	10.377	10.287	5.858	10.791	**11.226**

表 4 人人网数据集破解成功率

Table 4 Performance on renren test set

尝试次数	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
1000	11.599	10.933	7.067	11.640	**11.979**
2000	13.294	11.325	7.752	13.008	**13.544**
3000	14.184	12.757	8.273	14.160	**14.372**
4000	14.485	13.466	8.990	14.316	**14.808**
5000	14.990	13.949	9.103	14.677	**15.254**

在相同的破解次数下，对不同数据集实验结果如表 5~9 所示。可以看出来在不同的破解次数的条件下，本文提出的 PassCVAE 都取得了较好的结果。由于破解次数的增加，减少了生成破解的密码的随机性 PassCVAE 也会比其他对比算法表现的更加有优势，具有更高的破解成功率。

表 5 不同数据 1000 尝试次数破解成功率

Table 5 Performance on 1000 times

数据集	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
12306	1.364	2.025	1.049	2.227	**2.931**
CSDN	9.067	9.272	4.107	9.327	**9.497**
人人网	11.599	10.933	7.067	11.640	**11.979**

表 6 不同数据 2000 尝试次数破解成功率

Table 6 Performance on 2000 times

数据集	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
12306	1.984	2.153	1.170	2.880	**3.995**
CSDN	9.752	9.533	4.639	9.605	**9.960**
人人网	13.294	11.325	7.752	13.008	**13.544**

表 7 不同数据 3000 尝试次数破解成功率

Table 7 Performance on 3000 times

数据集	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
12306	2.355	3.515	1.706	3.394	**4.696**
CSDN	10.002	9.971	5.093	10.253	**10.382**
人人网	14.184	12.757	8.273	14.160	**14.372**

表 8 不同数据 4000 尝试次数破解成功率

Table 8 Performance on 4000 times

数据集	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
12306	2.616	3.761	1.714	3.856	**5.371**
CSDN	10.195	10.074	5.621	10.480	**10.978**
人人网	14.485	13.466	8.990	14.316	**14.808**

表 9　不同数据 5000 尝试次数破解成功率

Table 9　Performance on 5000 times

数据集	PCFG	OMEN	PassGAN	PassLSTM	PassCVAE
12306	3.280	4.282	1.746	4.282	**5.892**
CSDN	10.377	10.287	5.858	10.791	**11.226**
人人网	14.990	13.949	9.103	14.677	**15.254**

4　结束语

用户设置密码往往倾向于包含个人信息，而这种形式的密码更容易被密码攻击算法猜测到。本文基于条件变分自编码模型，将用户个人信息(邮箱地址、用户名、电话号码等)作为条件特征，训练密码攻击模型。在编码器端，分别使用双向 GRU 循环神经网络和 CNN 文本卷积神经网络，实现对密码序列和用户个人信息的编码和特征的抽象提取。在解码器端使用两层 GRU 神经网络，实现对用户个人信息和密码数据隐编码的解码生成密码序列。模型可以有效地拟合用户个人信息作为条件下的密码序列分布，实验表明本文所提出 PassCVAE 模型优于现有的主流密码攻击算法。

参考文献：

[1] Ma J, Yang Weining, Min Luo, *et al.* A study of probabilistic password models [C]//Proc of IEEE Symposium on Security and Privacy. San Jose: IEEE Press, 2014: 689-704.

[2] Dürmuth M, Angelstorf F, Castelluccia C, *et al*. OMEN: faster password guessing using an ordered Markov enumerator[C]**//Proc of International Symposium on Engineering Secure Software and Systems.** Berlin: Springer International Publishing, 2015: 119-132.

[3] Weir M, Aggarwal S, Medeiros B D, *et al.* Password cracking using probabilistic context-free grammars [C]//Proc of IEEE Symposium on Security & Privacy.Washington DC:IEEE Computer Society, 2009: 391-405.

[4] LeCun Y, Bengio Y, Hinton G. Deep learning [J]//Nature, 2015,521(7553): 436-436.

[5] Van Hasselt H, Guez A, Silver D. Deep reinforcement learning with double Q-learning [EB/OL].(2015-12-10).https://arxiv.org/pdf/1509.06461.pdf.

[6] Yu Lantao, Zhang Weinan, Wang Jun, *et al.* SeqGAN: sequence generative adversarial nets with policy gradient [EB/OL].(2017-08-28). https://arxiv.org/pdf/1609.05473.pdf.

[7] Lin K, Li Dianqi, He Xiaodong, *et al.* Adversarial ranking for language generation [C]//Advances in Neural Information Processing Systems. Cambridge: MIT Press, 2017: 3155-3165.

[8] Ding Wang, Zhang Zijian, Wang Ping, *et al.* Targeted online password guessing: An underestimated threat [C]//Proc of ACM SIGSAC Conference on Computer and Communications Security.New York: ACM Press 2016:1242-1254.

[9] Bauer L, Melicher W, Ur B, *et al.* Fast, lean, and accurate: Modeling password guessability using neural networks [C]//Proc of the 25th USENIX Security Symposium. Berkeley: USENIX Press, 2016:175-191.

[10] Hochreiter S, Schmidhuber J. Long Short-Term Memory [J]. Neural Computation, 1997, 9(8): 1935-1780.

[11] Karim F, Majumdar S, Darabi H, *et al.* LSTM fully convolutional networks for time series classification [J]. IEEE Access, 2018, 6(99): 1662-1669.

[12] Narayanan A, Shmatikov V. Fast dictionary attacks on passwords using time-space tradeoff[C]//Proc of ACM Conference on Computer and Communications Security.New York:ACM Press, 2005:364-372.

[13] Veras R, Collins C, Thorpe J. On the Semantic Patterns of Passwords and their Security Impact [C]//Proc of USENIX Networked and Distributed System Security Symposium. Berkeley,CA: USENIX Press, 2014:286-301.

[14] Li Zhigong, Han Weili, Xu Wenyuan. A large-scale empirical analysis of Chinese web passwords [C]//Proc of USENIX Conference on Security Symposium. Berkeley,CA: USENIX Press,2014:559-574.

[15] Bonneau J. The science of guessing: analyzing an anonymized corpus of 70 million passwords [C]// Security and Privacy. San Francisco: IEEE Press: 2012, 538-552.

[16] Castelluccia C, Dürmuth M, Perito D. Adaptive password-strength meters from markov models [C]//Proc of Usenix Networked and Distributed System Security Symposium. Berkeley,CA:USENIX Press: 2012, 143-156.

[17] Dell'Amico M, Filippone M. Monte Carlo Strength Evaluation: Fast and Reliable Password Checking [C]//Proc of ACM SIGSAC Conference on Computer and Communications Security. New York:: ACM Press,2015: 158-169.

[18] Ur B, Kelley P G, Komanduri S, *et al.* How does your password measure up?the effect of strength meters on password creation [C]// Proc of USENIX Security Symposium. Berkeley,CA:USENIX Press, 2012, 5-5.

[19] Hitaj B, Gasti P, Ateniese G, *et al.* PassGAN: a deep learning approach for password guessing [J]. arXiv preprint arXiv: 1709. 00440, 2017.

[20] Sohn K, Yan X, Lee H. Learning structured output representation using deep conditional generative models [C]//Proc of International Conference on Neural Information Processing Systems.Cambridge: MIT Press,2015: 3483-3491.

[21] Bao Jianmin, Chen Dong, Wen Fang, *et al.* CVAE-GAN: fine-grained image generation through asymmetric training [C]//Proc of IEEE International Conference on Computer Vision. Washington DC: IEEE Computer Society, 2017: 2764-2773.